Axxera

Predictive Security Solutions

Global Cyber Crime and Threat

June 11, 2009

Clifford Vazquez
Chief Technology Officer
Axxera Inc
www.axxera.net

Contents

WHY COMPANIES NEED MORE THAN A SECURITY PROCEDURES POLICY? 3

WHAT IS CYBER CRIME? 3

WHAT IS A DATA SECURITY BREACH? 3

DATA BREACH STATISTICS 4
DATA BREACH SOURCES 4
COST OF A SECURITY BREACH 5
DATA LOCATION AT THE TIME OF BREACH 6

LAWS TO COMBAT SECURITY BREACHES 6

PREDICTIVE PROACTIVE PROTECTION APPROACH 7

Why companies need more than a Security Procedures Policy?

Information technology has transformed the global economy and connected people and markets in ways never imagined. In order to realize the full benefits of the digital revolution, users must have confidence that sensitive information is secure, commerce in not compromised, and the infrastructure is not infiltrated.

The growing sophistication and breadth of criminal activity, along with the harm already caused by cyber incidents, highlight the potential for malicious activity in cyberspace to affect U.S competitiveness, degrade privacy and civil liberties protections, undermine national security, or cause a general erosion of trust, or even cripple society[1]. For example:

- **Failure of critical infrastructures**, caused by malicious activities against information technology systems have caused the disruption of electric power capabilities in multiple regions overseas, including a case that resulted in a multi-city power outage.
- **Exploiting global financial services**.
  - In November 2008, the compromised payment processors of an international bank permitted fraudulent transactions at more than 130 automated teller machines in 49 cities within a 30-minute period.
  - A U.S retailer in 2007 experienced data breaches and loss of personally identifiable information that compromised 45 million credit card and debit cards.
- **Systemic loss of U.S economic value**. Industry estimates of losses from intellectual property to data theft in 2008 range as high as $1 trillion

What is Cyber crime?

Cyber crime has been a problem since the late 1970's. With exponentially changing technology, cyber crime offenders are right there, keeping up with new ways to attack possible Internet victims.

Cyber crimes include, but are not limited to: identity theft, credit card fraud, cyber-stalking, phishing, and spoofing. Many types of cyber-crimes happen often through everyday emails, or in chat-rooms. Other types of cyber-crimes also involve software pirating, downloading illegal music files, and stealing money from banks by breaking into online websites.

What is a Data Security Breach?

When information falls into the wrong hands, or has had the opportunity to be extracted, viewed, captured, or used bay an unauthorized individual, it constitutes a data breach.

Data breaches can be classified into the following categories:

1. Data Breach
   - A hacker breaking in and downloading sensitive data
   - System(s) being infected with malicious software that captures, or sends sensitive data into criminal hands
   - Social engineering techniques whereby employees or other insiders are tricked into exposing sensitive information

[1] http://www.whitehouse.gov/CyberReview/

- Theft of computer systems, devices, or storage media that has sensitive data stored

2. Data Exposure
   - Sending sensitive information in emails
   - Posting sensitive information to a public forum such as a website
   - A computer glitch that causes the exposure of sensitive data
   - Sending sensitive information through the mail system in a way that is not secure.
   - Paper or other physical files that are placed in a public area that can be viewed or taken by unauthorized individuals
   - Not disposing of documents properly
3. Incidents concerning portable laptop computers, usually theft while away from the office (users home, car, or while travelling)
4. Loss of Media
   - Backup tapes, CDs, DVDs, or other storage medium lost
   - Computers or computer components that are donated or sold while sensitive information remains stored on the device.

Data Breach Statistics

According to laws in 40 of the 50 states, when a data security breach occurs, notification must be made to the affected individuals. Often, the exact number of compromised records or the number of affected individuals is unknown. This makes it difficult to quantify security breaches. Figure1 illustrates all publicly disclosed security breaches in the US between 2000 and 2007, where nearly one quarter of the incidents did not, or could not disclose the number of records that were part of their data security breach.

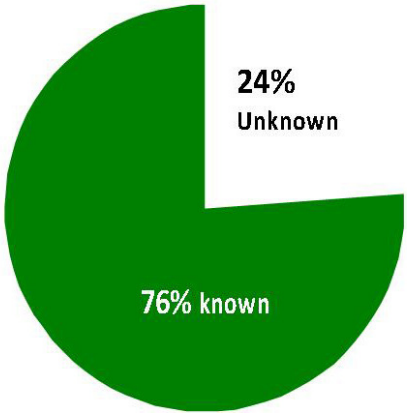

Figure 1. Number of Records Known vs Unknown

When a data security breach is discovered, and subsequent notifications are made, certain organizations maintain records of these breaches.[2] The data captured varies based on which organization is collecting it. Some only capture data for U.S based security breaches, while others capture data for international breaches. Most capture the name of the organization ad number of records compromised.

Data Breach Sources

The source of data breaches are broke down into the following segments as shown in figures 2 and 3

- Hacking
- Careless or Untrained User
- 3rd party
- Malicious Insider
- Theft

[2] http://www.attrition.org;http://privacyrights.org

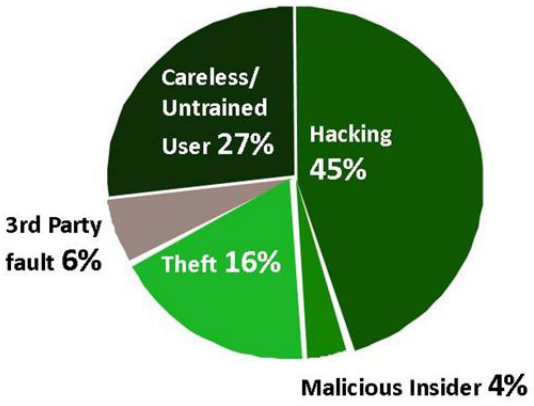

Figure 2: Incidents by Beach source

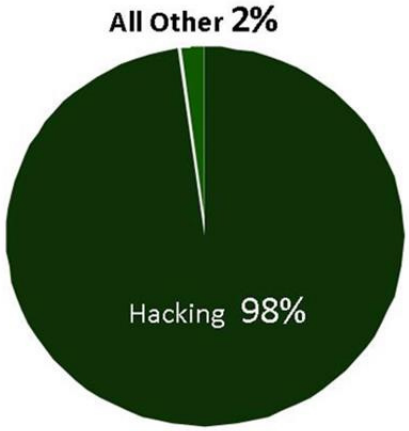

Figure 3: Records Compromised by Breach Source

Cost of a Security breach

The types of costs vary for several reasons including the type of company, industry, circumstances around the security breach, type of data compromised, liability, and the list goes on an. Many organizations are being required be federal law to perform risk assessments to determine their exposure to a variety of threats and risks. To perform a comprehensive rick analysis, an organization needs to know what it would cost to recover from a given compromise. Below are examples of costs associated with a security breach:

- Visa and TJX agree to provide U.S Issuers up to $40.9 million for data breach
- ChoicePoint settles data security breach charges; to pay $10 million in civil penalties, $5 million for consumer redress. At least 800 cases of identity theft arose from company's data breach[3]
- Data breach incidents cost companies $197 per compromised customer record in 2007 compared to $182 in 2006[4]
- A breach that exposes 46,000 identities will cost an organization $7.6 million on average[5]
- Forrester recently surveyed 28 companies that had data breaches and estimated that such a breach will cost an organization between $90 and $305 per exposed record, depending on the public profile of the breach and the regulations that apply to the organization[6]
- The average total cost per reporting company was $4.8 million per breach and ranged from $226,000 to $22 million[7]
- Lost productivity costs averaged $30 per lost record[8]
- The cost of new preventative measures averaged 4% of the total breach cost, or $180,000 on average[9]

Security Breach Impact on Small Organizations

It is usually not the fear, or reality of public backlash, but the hard and soft costs associated with recovering from a

[3] http://www.boston.com/news/local/maine/articles/2008/03/19/hannaford_hit_with_class_action_suit_in_data_breach_1205971643
[4] www.pgp.com/newsroom/mediareleases/ponemon-us.html
[5] http://www.news.com/8301-10784_3-6176074-7.html
[6] http://www.news.com/8301-10784_3-6176074-7.html
[7] www.computerworld.com/pdfs/PGP_Annual_Study_PDF.pdf
[8] www.computerworld.com/pdfs/PGP_Annual_Study_PDF.pdf
[9] www.computerworld.com/pdfs/PGP_Annual_Study_PDF.pdf

security breach that impacts small companies the most. In an Information Week article entitled "Companies Say Security Breach Could Destroy Their Business"[10] it states:

- One-third of companies said in a recent poll that a major security breach could put their company out of business
- A data breach that exposed personal information would cost companies an average of $268,000 to inform their customers—even if the lost data is never used
- 61% of respondents said data leakage is the doing of insiders, and 23% said those leaks are malicious
- 46% said they do not debrief or monitor employees after they give notice that they are leaving the company
- 23% said that they were able to estimate total annual cost of data leakage, putting the figure at $1.82 million.

Additionally, there have been cases where a security breach does cause a small company to go out of business. Verus Inc For example: "Medical IT Contractor Folds After Breaches-Blamed for privacy breaches at five different hospitals, Verus Inc. silently closes its doors."[11]

A study[12] from the Ponemon Institute found:

- Nearly one-third of people who were notified of a data security breach affecting personal information no longer conducted business with the company that suffered the breach
- 55% of respondents said they had been notified of more than one breach of data in the last two years
- 8% had received four or more breach notifications
- 63% of respondents said their notification letters offered no information about steps to take in order to protect their data
- More than half of the respondents said they were notified of breaches more than a month after the incident occurred
- Just 2% of respondents said they had been victims of identity fraud as a result of a data breach

Data Location at the Time of breach

Strong, enforced policies and procedures are not enough to stop all incidents. This is whetechnology solutions can be implemented to mitigate the risks. For example, if an employee inadvertently sends an email with sensitive information, that constitutes a security breach. If however, the organization has implemented an email content filtering solution that captured and quarantined that email, the incident has been averted. There are many ways in which secure, sensitive information can "leak" from an organization. Fortunately, there are many solutions available to address the variety of ways this can occur.

Laws to combat security breaches

In 2002, California signed the SB 1386 bill and the Data Breach Disclosure law became operative on July 1, 2003. Under this law any organization conducting business in California and processing personal information for California residents need to disclose any information security breach to California residents whose unencrypted personal information was obtained by an unauthorized person.

Following a high profile data security breach in 2005 involving ChoicePoint, and Cardsystems, many states used the SB 1386 bill as a model to help form their own security breach disclosure laws.

[10] http://www.informationweek.com/news/security/showArticle.jhtml;jsessionid=WoA23QSERJNEYQSNDLRSKHoCJUNN2JVN?articleID=199201085&_requestid=58557

[11] http://www.darkreading.com:80/document.asp?doc_id=131712

[12] http://www.darkreading.com/document.asp?doc_id=151378

Demonstrating commitment to cyber security-related issues at the highest levels of government, industry, and civil society will allow the United States to continue to lead innovation and adoption of cutting-edge technology, while enhancing national security and the global economy.

A growing array of state and non-state actors are targeting US citizens, commerce, critical infrastructure, and government. These actors have the ability to compromise, steal, change, or completely destroy critical information.

Predictive Proactive Protection Approach

Sophisticated hacker attacks take time to develop and are usually launched in stages using botnets. Most organizations ignore the seemingly harmless non-threatening scans circulating on the Internet. However, these threats are often the building blocks of a more concentrated, potentially devastating attack. Using a progressive threat model, allows predictive security approach to correlate more sophisticated actions with the earlier activities to help identify which combinations of attacks require immediate action, and prevent the attack.

Using global threat intelligence from sensors across the internet, this reputation based service continually updates customers backbone routers with a personalized global threat lists to prevent inbound and outbound connection to malware sources and botnet controllers.

A well implemented internet security intelligence stop the most active botnets from spreading virus, spam, phishing, DDOS attacks and exploiting harvesting bots in your network. Intelligence based protection and traffic redirection technologies help the proactive reaction to the cyber attack.

If your network has a compromised system, when it tries to communicate with its botnet, your core router protects and blocks the connection pro-actively. This stops any data leakage and lets you assure good reputation IP addresses communicate through your network.

Using global real time statistics and global law enforcement intelligence we enable our customers to filter their traffic based on reputation. Intelligence working together with software to protect your critical information assets.

For more information on this topic and thoughts on how to protect your organization contact author, or visit www.axxera.net